AMENDMENT

In the Claims

1. (Currently Amended) A computer-implemented method for gathering security event data and rendering result data in a manageable format comprising the steps of:

generating a plurality of alerts with a plurality of security devices at a first location;

providing one or more variables operable for analyzing and filtering security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event;

creating scope criteria by ~~adjusting~~ selecting one or more of the variables operable for analyzing and filtering security event data, the security event data comprising the plurality of alerts;

collecting the security event data generated by the plurality of security devices located at the first location;

storing the collected security event data at a second location; [[and]]

analyzing and filtering the collected security event data with the scope criteria to produce result data, ~~the result data accessible by a plurality of clients~~.

transmitting the result data to one or more clients; and

displaying the result data comprising filtered alerts based on the scope criteria.

2. (Original) The method of Claim 1, further comprising storing one or more of the scope criteria and the result data.

3. (Original) The method of Claim 1, wherein the first location is a distributed computing environment and the second location is a database server.

4. (Original) The method of Claim 1, wherein collecting the security event data comprises

generating security event data from a sensor;
sending the security event data from the sensor to a collector; and
converting the event data to a common format.

5. (Original) The method of Claim 1, wherein the analyzing is performed at an application server to which the plurality of clients are coupled

6. (Original) The method of Claim 1, further comprising searching the stored security event data for additional information identifying a security event.

7. (Original) The method of Claim 1, further comprising:
polling a database server for current stored security event data;
analyzing the current stored security event data to produce current result data; and
rendering the current result data.

8. (Original) The method of Claim 1, further comprising polling for messages containing information about scope criteria, security event data, or result data.

9. (Original) The method of Claim 1, further comprising pushing messages to a client wherein the messages contain information about scope criteria, security event data, or result data.

10. (Original) The method of Claim 1, wherein the step of rendering result data comprises presenting the result data in a chart format.

11. (Original) The method of Claim 1, wherein in response to analyzing the collected security event data, an action is executed.

12. (Original) The method of Claim 11, wherein the action is clearing security event data from storage.

13. (Original) The method of Claim 11, wherein the action is creating an incident from result data for preparing a response.

14. (Original) The method of Claim 1, wherein the step of collecting security event data further comprises converting the data to a uniform format.

15. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 1.

[The Remainder of this page has been intentionally left blank.]

16. (Currently Amended) A method for managing security event data collected from a plurality of security devices in a distributed computing environment comprising the steps of:

generating a plurality of alerts with the plurality of security devices at a first location;

providing one or more variables operable for analyzing and filtering security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event;

creating scope criteria by adjusting selecting one or more of the variables operable for analyzing and filtering security event data, the security event data comprising the plurality of alerts;

collecting security event data at a second location; [[and]]

applying the scope criteria to the security event data at a third location to produce [[a]] result data, ~~the result accessible by a plurality of clients coupled to~~ a server.;

transmitting the result data to one or more clients; and

displaying the result data comprising filtered alerts based on the scope criteria.

17. (Original) The method of Claim 16, further comprising rendering the result in a rendering for output to a client.

18. (Original) The method of Claim 16, wherein the first location is a distributed computing environment.

19. (Original) The method of Claim 16, wherein the second location is a database server.

20. (Original) The method of Claim 16, wherein the third location is an application server coupled to the plurality of clients.

21. (Original) The method of Claim 16, further comprising storing one or more of the scope criteria, the security event data, and the result in a database.

22. (Original) The method of Claim 16, further comprising executing an action at the server in response to producing the result.

23. (Original) The method of Claim 22, wherein the action is clearing stored security event data.

24. (Original) The method of Claim 22, wherein the action is creating an incident from a result.

25. (Original) The method of Claim 16, further comprising applying additional scope criteria to a plurality of results.

26. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 16.

[The Remainder of this page has been intentionally left blank.]

27. (Currently Amended) A computer-implemented system for managing security event data collected from a plurality of security devices comprising:

a plurality of security devices operable for generating security event data comprising a plurality of alerts;

an event manager coupled to the security devices, the event manager operable for collecting security event data from the security devices and analyzing and filtering the security event data with scope criteria comprising ~~a plurality of~~ one or more definable variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event, and the event manager operable for applying the scope criteria to the security event data to produce result data; and

~~a client~~ one or more clients coupled to the event manager operable to perform an action in response to receiving analyzed security event data from the event manager and displaying the result data comprising filtered alerts based on the scope criteria.

28. (Previously Amended) The system of Claim 27, wherein the event manager comprises a database server operable for storing the collected security event data and the analyzed security event data.

29. (Original) The system of Claim 27, wherein the event manager comprises an application server operable for creating an incident from the security event data for preparing a response.

30. (Original) The system of Claim 27, wherein the security devices are coupled to a distributed computing network.

31. (Original) The system of Claim 27, wherein multiple clients operable for receiving analyzed security data are coupled to the event manager.

32. (Original) The method of Claim 27, wherein the action performed by the client is rendering a chart containing analyzed security event data.

33. (Original) The method of Claim 1, further comprising the step of rendering the result data in a manageable format for the plurality of clients.

[The Remainder of this page has been intentionally left blank.]

34. (Currently Amended) A computer-implemented method for gathering security event data and rendering result data in a manageable format comprising the steps of:

generating a plurality of alerts with a plurality of security devices at a first location;

providing one or more variables operable for analyzing and filtering security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event;

creating scope criteria by ~~adjusting~~ selecting one or more of the variables operable for analyzing and filtering security event data, the security event data comprising the plurality of alerts;

collecting the security event data at a second location;

analyzing and filtering the collected security event data with the scope criteria at a third location to produce result data, ~~the result~~ data accessible ~~by a plurality of clients; and~~

transmitting the result data to one or more clients; and

rendering the result data, in a manageable format for the ~~plurality of~~ one or more clients.

35. (Original) The method of Claim 34, further comprising storing one or more of the scope criteria, the security event data, and the result data.

36. (Original) The method of Claim 34, wherein the first location is a distributed computing environment, the second location is a database server, and the third location is an application server to which the plurality of clients are coupled.

37. (Original) The method of Claim 34, further comprising editing the scope criteria.

38. (Original) The method of Claim 34, further comprising converting the collected security event data to a common format.

39. (Original) The method of Claim 35, further comprising searching the stored security event data for additional information identifying a security event.

40. (Original) The method of Claim 35, further comprising:
polling a database server for current stored security event data;
analyzing the current stored security event data to produce current result data; and
rendering the current result data.

41. (Original) The method of Claim 34, further comprising polling for messages containing information about scope criteria, security event data, or result data.

42. (Original) The method of Claim 34, further comprising pushing messages to a client wherein the messages contain information about scope criteria, security event data, or result data.

43. (Original) The method of Claim 34, wherein the step of rendering the result data comprises presenting the result data in a chart format.

44. (Original) The method of Claim 34, wherein in response to analyzing the collected security event data, an action is executed.

45. (Original) The method of Claim 44, wherein the action is clearing security event data from storage.

46. (Original) The method of Claim 44, wherein the action is creating an incident from result data for preparing a response.

47. (Original) The method of Claim 34, wherein the step of collecting security event data further comprises converting the data to a uniform format.

48. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 34.

[The Remainder of this page has been intentionally left blank.]

49. (Currently Amended) A method for managing security event data collected from a plurality of security devices in a distributed computing environment comprising the steps of:

generating security event data with a plurality of security devices, the security event data comprising a plurality of alerts;

transferring the security event data for storage in a database;

applying a scope criteria comprising ~~a plurality of~~ one or more defineable variables to the security event data for analyzing and filtering the security event data to produce a result, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event; [[and]]

accessing the result with one or more clients coupled to an application server; and

displaying the result data comprising filtered alerts based on the scope criteria.

50. (Original) The method of Claim 49, further comprising rendering the result in a rendering for output to the clients.

51. (Original) The method of Claim 49, further comprising the step of creating the scope criteria for filtering the security event data.

52. (Original) The method of Claim 49, further comprising the step of editing the scope criteria.

53. (Original) The method of Claim 49, further comprising converting the security event data to a uniform format.

54. (Original) The method of Claim 49, further comprising storing one or more of the scope criteria, the security event data, and the result in a database.

55. (Original) The method of Claim 49, wherein in response to producing a result, an action is executed.

56. (Original) The method of Claim 55, wherein the action is clearing stored security event data.

57. (Original) The method of Claim 55, wherein the action is creating an incident from a result.

58. (Original) The method of Claim 49, further comprising applying additional scope criteria to a plurality of results.

59. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 49.

[The Remainder of this page has been intentionally left blank.]